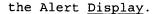# WEST Search History

| Hide Items | Restore | Clear | Cancel |

DATE: Saturday, May 15, 2004

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=ADJ	
☐	L19	6513129.pn. and display$	1
☐	L18	L17 and ((severe or severity) near3 level)	3
☐	L17	(6513129 or 6505245 or 6481005).pn.	3
☐	L13	(severe or severity) near3 level near3 chang$	46
☐	L12	L11.ti.	1
☐	L11	L10 or l7	213
☐	L10	sever$ near3 level near5 dynamic$	33
☐	L7	sever$ near3 level near3 chang$	180
☐	L6	L4.ti,ab.	11
☐	L5	L4 near10 dynamic$	1
☐	L4	alert$ near5 detect$ near5 (event or situation)	210
☐	L2	5528516[uref]	44
☐	L1	5528516.pn.	1

END OF SEARCH HISTORY

the Alert Display.

Detailed Description Text (37):
The control object contains attributes that dictate system response to an incoming alarm. Basic functionality such as alert generation, logging, forwarding is described by the control object itself. Initiation of advanced functions (e.g., Suppression, Escalation, Correlation, and Thresh-holding) are handled through scenario objects initiated by a control object. Finally, the alarm incident is processed and FMS 400 responds in accordance with the pre-defined policies of the system (e.g., display fault alert).

Detailed Description Text (43):
The Clear Type attribute 521 is used to control alert clearance behavior. Its possible values include ACK, MAN, RESET, and FULL with its default being RESET. ACK causes the alert to clear from the system on receipt of a clear indication from the equipment only if the alert was manually acknowledged. If unacknowledged, the alert severity will be set to indeterminate when the clear is received. MAN causes any clear messages received from the Element Manager or device to be ignored. These alerts should always be manually cleared. RESET causes the alert severity to be set to "indeterminate" when a clear for the alert is received. The indeterminate event must then be manually selected and cleared to remove it from the Alert Display. FULL causes the alert to fully clear from the Alert Display.

Detailed Description Text (49):
The Log Alert attribute 533 is used to control alert logging behavior. Its possible values are 0, 1, and 2 with a default value of 2.0 means do not log the alert details when this control object triggers system response. 1 means log the alert details only if the alert is generated on the Alert Display. 2 means always log the alert details.

Detailed Description Text (52):
The Manual Clear attribute 539 is of boolean type with a default of True. If True, the alarm incident is permitted to be cleared manually. This is used to control manual clearance behavior. If this box is checked, manual clearance is permitted. Note that for correlation alerts, manual clear should be True only if the alert needs to be manually cleared in exceptional circumstances. If an alert is selected on the Alert Display to be manually cleared, and the value is False, the alert will remain on the alert display.

Detailed Description Text (66):
When an incoming alarm incident completes a predefined alarm pattern, a new "correlation" alert is generated on an Alert Display Window at the display terminal interface 445. All alerts comprising the alert pattern are then temporarily removed from the Alert Display Window. While the correlation alert is active, subsequent alarms which match the correlation pattern of the correlation alert are not displayed.

Detailed Description Text (67):
Correlation alerts should not be manually cleared. When an "alarm clear" for one of the alerts comprising the underlying correlation alert pattern is received from the EM or device, the "correlation" alert is automatically cleared from the Alert Display Window, if the Auto Clear attribute is set to True. The remaining alerts that were temporarily removed from the Alert Display, or which were suppressed before being generated as a result of the correlation alert being present, are regenerated. If the Auto Clear attribute is set to False, the underlying alerts will not be regenerated when the correlation alert pattern is no longer active.

Detailed Description Text (70):
When an alarm is received on one end, and if AND is selected for the present conditions, the other end is checked for the same alarm, or the alarm specified in

First Hit   Fwd Refs

L6: Entry 3 of 11   File: USPT   Aug 20, 2002

DOCUMENT-IDENTIFIER: US 6438696 B1
TITLE: Security monitoring arrangement for a computer system

Abstract Text (1):
An electronic point-of-sale (PoS) system comprises a network with a number of PoS terminals and a PoS server computer attached to it. The PoS terminals and the PoS server interact over the network to perform conventional PoS transactions. Additionally, each of the PoS terminals monitors its own operation for predetermined security-related events (such as refunds or voids). Upon detection of such an event, the PoS terminal sends an alert message and data over the network to a control computer (which may be the PoS server computer, or may be a separate computer). The control computer responds to the alert message by activating a video camera and recorder to record a view of the PoS terminal, along with the data.

First Hit   Fwd Refs

☐ | Generate Collection |

L13: Entry 10 of 46   File: USPT   Nov 12, 2002

DOCUMENT-IDENTIFIER: US 6481005 B1
TITLE: Event correlation feature for a telephone network operations support system

Detailed Description Text (28):
As another example, the claimed invention can be adapted so that alarms that are
correlated together have an aggregate severity level. Typically, an individual
alarm has a severity level associated with it (for example critical, major, or
minor). Because alarms that are correlated together are related to a common fault
condition, it is useful that all alarms in a tree have the same severity level.
Correlation rules can be written so that the individual severity level of each
alarm in a given correlation tree can be changed to be the same as the most severe
level of all alarms in that tree.

CLAIMS:

3. The method of claim 2 wherein said messages are associated with respective
errors ranging from most severe to least severe and wherein said step of adding
includes the step of changing the level of severity associated with said received
message when it is added to each of said identified groups to the level of the
message having the highest level of severity in that group.

Hit List

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: US 6513129 B1

L19: Entry 1 of 1   File: USPT   Jan 28, 2003

DOCUMENT-IDENTIFIER: US 6513129 B1
** See image for <u>Certificate of Correction</u> **
TITLE: System and method for managing faults using a gateway

<u>Detailed Description Text</u> (16):
User interface 245 may be any suitable device (or devices) such as a <u>display</u>
terminal for providing users with interactive access to the management system 200
through gateway 225 and/or management processors 230A, 230B, 230C, 230D. As
discussed above, the user interface may actually comprise a plurality of user
interfaces depending upon the particular requirements of the managed network.

<u>Detailed Description Text</u> (28):
FMS 400 generally includes gateway 425, fault management processor system 430, and
<u>display</u> terminal interface 445 for <u>displaying</u> to a user fault alerts (via an Alert
<u>Display</u>) and for receiving from the user appropriate command and configuration
information. Topological representations of the network and its state may also be
included. Gateway 425 is interconnected between management processor system 430 and
the network elements 210 for receiving incoming fault incidents from network
elements and element managers. <u>Display</u> terminal interface 445 is connected to both
the gateway 425 and the management processor system 430. In one preferred
embodiment, gateway 425 actually comprises a plurality of distributed gateways.
Accordingly, the <u>display</u> terminal interface comprises several <u>display</u> terminals for
servicing the fault management processor system 430.

<u>Detailed Description Text</u> (29):
FIG. 7 diagrammatically depicts the processing flow of an incoming alarm incident.
In operation, the network element 210 sends a raw alarm incident to the gateway 425
where it is received at gateway interface 426. It is passed to a normalization rule
engine at 427 where it is normalized; that is, identification and parse rules are
applied in order to translate it from a vendor specific form into a form that is
amenable for processing throughout the system. Based on data from this normalized
incident, the gateway 425 then selects at 428 the "closest" control object 465 and
processes it. In doing so, the rule engine selects the control object whose name
most closely matches the normalized incident data. Once the control object is
selected, the attributes in the control object determine how the alarm incident
will be processed. In some cases, advanced processing in the management processing
system 430 will be required. The processed control object may cause one or more
other control objects 467 and/or any necessary scenario objects 469 (e.g., for
performing correlation or suppression) to be processed. The management processing
system 430 would then take appropriate action such as <u>displaying</u> alert information
on the <u>display</u> terminal interface 445. In other cases, the basic processing in the
gateway 425 may directly cause, for example, an alert message to be <u>displayed</u> on

the correlation scenario. (The other end is identified through a lookup table entry). If AND was specified and the conditions of the circuit correlation alarm are met, both alerts are hidden and a new alert is generated to indicate that the link (or circuit) is in alarm. If OR was specified, then the correlation alert will be generated whether or not the other end alert has been received. In this case, if the other end alert is received after the correlation alert has triggered, this alert will not be displayed, but will be regenerated when the correlation condition is no longer active (and Auto Clear is True), and if this alert has not been cleared in the meantime.

Detailed Description Text (85):
Setting Threshold parameters allows alarm incidents that occur often to generate alerts on the Alert Display only when a certain number of alarms are received within a given time interval. In other words, when they reach a preset threshold. This is known as rate thresholding. Thresholding can also count the number of alert clears that are received in a given time before an alert is generated, this is fleeting Thresholding.

Detailed Description Text (90):
There are two standard thresholding methods: rate thresholding and fleeting thresholding. Rate thresholding is handled by suppressing the number of alarms that are received until the threshold is reached for the alarm that is being thresholded, and then generating the threshold alert. This type of threshold can escalate or de-escalate because each clear received subtracts from the count of alarms. Different high-water marks can cause different severities to be applied to the alarm. Alarm clears are always recognized in threshold processing whether the Clear Type is set to manual or not. If an alert already exists on the Alert Display for the previous threshold--according to the internal threshold count--the severity level is adjusted as required, or if the threshold requirement is no longer satisfied for any severity level, the alert is removed from the Alert Display. Three ways for clearing a rate threshold include Clearing the threshold rate manually, automatically clearing when enough clears are received to bring the threshold level down to the lowest preset level, and automatically clearing when there are not enough alarms received during a preset interval of time and a new alarm of the specified type is received.
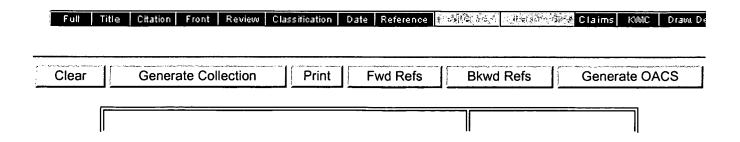
Detailed Description Text (123):
Suppression causes specified alerts to be permanently removed from the Alert Display window when a suppressor alarm is received.

Detailed Description Text (124):
While the suppressor alert is active, subsequent alarms that match the suppression pattern do not display on the Alert Display Window.

CLAIMS:

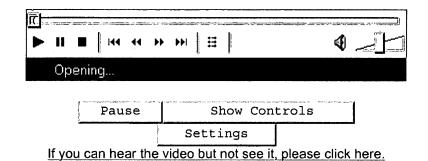2. The system of claim 1 further comprising an alert display operably connected to the system for displaying to a user alert information.

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D |

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS |

Terms	Documents
6513129.pn. and display$	1

Display Format: KWIC | Change Format |

Previous Page   Next Page   Go to Doc#

Pause | Show Controls

Settings

If you can hear the video but not see it, please click here.

☐ | Generate Collection |

L13: Entry 7 of 46   File: USPT   Jan 28, 2003

DOCUMENT-IDENTIFIER: US 6513129 B1
** See image for Certificate of Correction **
TITLE: System and method for managing faults using a gateway

Detailed Description Text (88):
If additional alarms are received such that the threshold requirements for a higher
severity level are satisfied, the severity of the alert is changed to reflect the
new specified value. Clears will similarly decrement the count and severity level
as a previous threshold is reached.

First Hit   Fwd Refs

☐   Generate Collection

L13: Entry 8 of 46   File: USPT   Jan 7, 2003

DOCUMENT-IDENTIFIER: US 6505245 B1
TITLE: System and method for managing computing devices within a data
communications network from a remotely located console

Detailed Description Text (79):
FIG. 21 shows an example screen for changing the severity levels and colors for the
error messages.